(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
G06F 17/60D0

(11) 공개번호 특2002-0063534
(43) 공개일자 2002년08월03일

(21) 출원번호 10-2002-0035691
(22) 출원일자 2002년06월25일

(71) 출원인 디프소프트 주식회사
서울특별시 강남구 역삼동 837-33 영플레이스빌딩 4층
(72) 발명자 하정호
경기도성남시분당구금곡동청솔주공아파트904동801호
안재근
경기도성남시수정구태평1동7254-1삼보주택가동302호
정기철
서울특별시관악구봉천1동968-3501호
김형은
인천광역시부평구산곡1동177-69현대아파트201동2001호
(74) 대리인 김희소, 김봉희

심사청구 : 있음

(54) 스팸메일 필터링 방법

요약

본 발명은 전자메일을 지원하는 네트워크 시스템, 서버 및 CGI(Common Gateway Interface)에 있어서 스팸메일을 차단하는 스팸메일 필터링 방법에 관한 것으로서, 본 발명에 따른 스팸메일 필터링 방법은: 전자메일 처리 시스템에서 스팸메일을 필터링하는 방법에 있어서, 상기 전자메일 처리 시스템을 통하여 송/수신되는 메일을 스팸메일의 헤더조건에 따라 차단하는 메일헤더 필터링 과정과, 상기 메일헤더 필터링된 메일을 스팸메일의 본문조건에 따라 차단하는 메일본문 필터링 과정과, 상기 메일본문 필터링된 메일을 스팸메일의 연결수조건에 따라 차단하는 연결 필터링 과정과, 상기 연결 필터링된 메일을 스팸메일의 SMTP명령어 조건에 따라 차단하는 SMTP명령어 필터링 과정과, 상기 SMTP명령어 필터링된 메일을 바이러스 검사 및 치료하는 과정을 적어도 구비함을 특징으로 한다.

대표도

도8

색인어

전자메일, 스팸, 필터링

명세서

도면의 간단한 설명

도 1은 본 발명이 적용되는 네트워크 환경에서 스팸 처리 엔진을 포함하는 전자메일 처리 시스템을 도시한 도면,

도 2a는 본 발명의 일 실시 예에 따른 스팸 처리 엔진의 개념도,

도 2b는 본 발명의 다른 실시 예에 따른 스팸 처리 엔진의 개념도,

도 3은 본 발명의 바람직한 실시 예에 따른 전자메일 처리 시스템의 계층 구성을 도시한 도면,

도 4는 본 발명의 바람직한 실시 예에 따른 웹서버의 내부 구성을 도시한 도면,

도 5는 본 발명의 바람직한 실시 예에 따른 스팸메일 처리를 위한 데이터베이스의 구성을 도시한 도면,

도 6은 본 발명의 바람직한 실시 예에 따른 전자메일 처리 시스템에서 메일 수신 서비스를 도시한 도면,

도 7은 본 발명의 바람직한 실시 예에 따른 전자메일 처리 시스템에서 메일 발송 서비스를 도시한 도면,

도 8은 본 발명의 바람직한 실시 예에 따른 전자메일 처리 시스템에서 스팸 필터링 과정을 도시한 도면.

* 도면의 주요 부분에 대한 부호의 설명 *

10: 클라이언트 서버20: 사용자1

30: 사용자n40: 인터넷 or LAN

100: 플랫폼200: 웹서버

210: 웹서버 처리부220: 스팸 처리 엔진

221: 스팸 처리부222: 메일헤더 필터링부

223: 메일본문 필터링부224: 메일연결 필터링부

225: SMTP명령어 필터링부227: 필터링엔진 자동업그레이드부

229: 관리자도구230: 바이러스 검출엔진

300: 메일서버400: 데이터베이스

410: 스팸메일 정보 데이터베이스411: 스팸메일헤더정보 데이터베이스

412: 스팸메일본문정보 데이터베이스

413: 스팸메일 연결수정보 데이터베이스

414: 스팸메일 SMTP명령어정보 데이터베이스

420: 바이러스메일 정보 데이터베이스

430: 정상메일 정보 데이터베이스440: 사용자 정보 데이터베이스

450: 메시지 저장 데이터베이스 460: 첨부파일 저장 데이터베이스

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 이-메일이라 일컬어지는 전자메일(Electronic Mail: E-Mail) 처리 기술에 관한 것으로, 특히 전자메일을 지원하는 네트워크 시스템, 서버 및 CGI(Common Gateway Interface)에 있어서 스팸메일을 차단하는 스팸메일 필터링 방법에 관한 것이다.

1999년부터 급속히 늘어난 인터넷 이용자 확산과 시장규모의 급증에 따라 현재 인터넷은 사회, 경제, 문화 등 사회 전반에 엄청난 영향을 끼치고 있으며, 이와 관련된 인터넷과 주요 이슈가 회자되고 있다. 특히 일반 가정에까지 초고속 통신망 및 무선 인터넷의 보급 확대는 인터넷이라는 보이지 않는 거대한 시장을 창출하여 벤처 기업의 급증과, 전자 상거래의 촉진, 인터넷 광고 시장의 활성화 등 신경제의 핵심 기반이 되고 있다. 이러한 인터넷 인프라의 확충은 양질, 대용량의 컨텐츠를 보다 빠르고 쉽게 이용할 수 있도록 하며, 향후 진보된 생활과 산업 창출의 기반 시설이 될 것이 현재로서는 확실해 보인다.

이러한 인터넷 서비스 중에서 가장 널리 사용되는 서비스로 전자메일 서비스를 들 수 있다.

전자메일 서비스는 인터넷에서 가장 먼저 사용되었으면서도 또한 아직까지 가장 활발하게 이용되고 있는 서비스 중의 하나이다. 전자메일 서비스는 전화와 달리 수취인의 부재와 관계없이 편지를 보낼 수가 있고 받는 상대뿐만 아니라 보내는 사람이 원할 때에 보낼 수 있으며, 파일을 첨부파일의 형태로 보낼 수도 있다. 또한 같은 내용의 편지를 많은 사람에게 동시에 보내고자 하는 경우에도 수신처를 복수로 지정하거나 미리 그룹화 시켜서 간단히 처리할 수 있다.

현재 3억2천5백만 이상의 전자메일박스가 사용되고 있으며 매년 60%씩 증가하는 전자메일은 1998년에 총 78조개의 전자메일 메시지가 송/수신되었으며 2003년에는 452조개의 전자메일 메시지가 송/수신될 것으로 예측된다. 또한 사용자당 전자메일 메시지의 전송률이 매년 2배씩 증가하는 추세에 있다.

이러한 전자메일의 기하급수적인 증가에 따라 이를 통하여 자사의 제품을 홍보하고자 하는 상업성 광고메일이 홍수를 이루고 있으며, 전자메일의 특성을 이용하여 불법적인 목적을 달성하고자하는 불법적인 시도가 이루어지고 있다. 따라서 이러한 원하지 않는 광고메일이나 바이러스메일로 인하여 전자메일 시스템을 이용하는 사용자들이 정신적, 물적인 피해를 입게 되는 사례가 급증하고 있다.

상기한 바와 같이 우리가 원하지도, 요청하지도 않았는데 어쩔 수 없이 받는 불필요한 메일을 스팸(Spam)메일, 정크(Junk)메일 또는 벌크(Bulk)메일이라고 한다. 이러한 스팸메일은 원하지 않는 전자메일 사용자

들에게 단순히 시간을 낭비하게 만드는 상업적 광고메일들뿐만 아니라, 수신 취소가 어렵거나 아예 수신 취소를 할 수 없는 광고메일, 피라미드 사기메일, 행운의 편지, 탄드라 토템 등 수신인에게 공포심 불안감을 유발함으로서 메일 보내기를 유도하여 네트워크나 서버 사용량을 증대시켜 속도를 느리게 하는 메일, 돈버는 사이트 소개메일, 기타 인터넷 상의 특정 사용자에게 복수를 하거나 괴롭히기 위하여 보내는 같은 내용의 메일 또는 사이즈가 큰 메일, 메시지를 열어보거나 작동시킬 때 상대방의 시스템을 손상시킬 목적으로 바이러스 등을 첨부하여 보내는 메일, 기타 외설 또는 폭력적인 메시지·화상·음성 등이 담긴 공서양속에 반하는 메일을 모두 포함한다.

이러한 스팸메일이 급증하면서 전자메일을 제공하고 있는 대부분의 포탈 사이트의 웹 기반의 웹메일을 제공하는 서버와, 메일 클라이언트를 이용한 POP#N(Post Office Protocol version N, 현재는 POP3 서비스) 서비스를 제공하기 위한 서버에 부하가 폭주하여 서버 접속 불능 등 처리 과부하가 걸리는 현상이 잦아지고 있으며, 속도 지연 등의 문제를 일으키고 있다.

이를 위하여 해당 관리자들은 저마다 대용량의 서버환경을 서둘러 마련하여 동시 대량 메일에 의한 폭주로 인한 접속 불능, 속도 지연 등의 이용자 불편 사항을 처리하고 있으나, 서버 용량을 무한정 늘리는 것은 스팸메일에 대한 근본적인 대책이 되지 못한다.

또한, 스팸메일로 인한 피해와 문제점을 해결하기 위해 웹메일을 제공하는 사업자들을 중심으로 특정 도메인 또는 IP주소들이 발송하거나 중계하는 메일, 특정 사이트 또는 사용자들이 발송하는 메일, 원치 않는 메일들이 폭주하는 내부계정으로부터의 메일을 차단하고, 사용자가 수신 취소를 한 스팸메일에 대하여 이후 동일한 메일이 수신되지 않도록 사용자들로부터 수신 거부되거나 수신 취소된 메일의 해당 발송 주소를 수신거부리스트에 등록하거나, 이러한 사용자들의 스팸신고를 참조하는 스팸걸러내기 기능을 제공을 차단하는 방법들이 사용되고 있다.

한편, 전자메일의 대부분을 차지하고 있는 상업성 광고메일에 대하여, 대량으로 메일을 발송하는 업체들이 실명으로 메일을 발송하도록 온라인 우표를 발행함으로서 대량의 메일을 생산하는 업체 스스로가 책임감을 갖고 건전한 메일만을 발송하도록 유도하며, 스팸발생 업체에 대해서는 실명정보를 바탕으로 효과적인 처벌이 가능하도록 하는 방법도 사용되고 있다. 즉, 온라인 우표를 발행함으로써 문제가 있는 메일을 발송하는 업체를 미연에 차단하고, 사용자의 정보성 또는 상업성 평가에 따라 적정한 비용을 부담케하며, 메일발송통수에 따라 우표를 구매토록 하여 많은 메일에 대해서는 더 많은 요금을 부담케 함으로써 무분별한 메일 발송을 차단하며 스팸메일을 감소시키는 누적과금제를 적용한 장벽방식이다.

그러나 이러한 온라인 우표를 발행하여 스팸메일을 차단하는 방법은 대량의 메일(예로써, 일회 발송 시 1000통 이상)을 발송하거나, 대량의 메일이 수신되는 다수의 사용자를 보유하고 있는 대규모의 웹메일 사이트나 메일서버에서는 효과적일 수 있으나, 보통의 웹메일 서비스 서버, 메일 서버/클라이언트를 이용하는 메일서버에서의 온라인 우표 발행은 무의미할 뿐만 아니라 실질적으로 불가능하다.

상기한 바와 같이 계속적으로 늘어만 가는 스팸메일에 대한 해결책으로서, 서버 용량을 무한정 늘리거나, 온라인 우표를 발행하는 것은 근본적이고 일반적인 해결 방법이 되지 못한다.

따라서 기존 전자메일서버의 시스템 환경 내에서 처리메일의 부하를 최소화하도록 스팸메일을 최대한 필터링함으로써, 메일서버의 접속 불능이나 속도 지연을 최소화 할 수 있는 스팸메일 차단 방법이 요망된다.

발명이 이루고자 하는 기술적 과제

따라서, 본 발명의 목적은 전자메일 처리 시스템에서 송/수신되는 메일을 처리하는 메일서버의 부하를 최소화할 수 있도록 메일서버에 스팸메일을 폭넓게 차단할 수 있는 방화벽을 제공하는 스팸메일 필터링 방법을 제공함에 있다.

발명의 구성 및 작용

상기의 목적을 해결하기 위하여 본 발명의 바람직한 실시 예에 따른 전자메일 처리 시스템에서의 스팸메일 필터링 방법은: 상기 전자메일 처리 시스템을 통하여 송/수신되는 메일을 스팸메일의 헤더조건에 따라 차단하는 메일헤더 필터링 과정과, 상기 메일헤더 필터링된 메일을 스팸메일의 본문조건에 따라 차단하는 메일본문 필터링 과정과, 상기 메일본문 필터링된 메일을 스팸메일의 연결수조건에 따라 차단하는 연결 필터링 과정과, 상기 연결 필터링된 메일을 스팸메일의 SMTP명령어조건에 따라 차단하는 SMTP명령어 필터링 과정과, 상기 SMTP명령어 필터링된 메일을 바이러스 검사 및 치료하는 과정을 적어도 구비함을 특징으로 한다.

이때, 상기 연결 필터링 과정은, 상기 전자메일 처리 시스템이 다수의 메일발송을 동시에 시도하는 동시연결수에 대한 제한조건과, 상기 전자메일 처리 시스템이 단일시간당 동일한 메일발송을 반복적으로 시도하는 단위시간당 연결수에 대한 제한조건에 따라 필터링을 수행함을 특징으로 하며, 상기 전자메일 처리 시스템을 유지 및 보수하기 위한 관리자도구를 통하여 상기 모든 필터링 조건의 추가변경이 가능함을 특징으로 한다.

이하 본 발명의 바람직한 실시 예를 첨부한 도면을 참조하여 상세히 설명한다. 우선 각 도면의 구성 요소들에 참조부호를 부가함에 있어서, 동일한 구성 요소들에 한해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 그리고 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 공지 기능 및 구성에 대한 상세한 설명은 생략한다. 한편, 이하에 설명하는 본 발명에 따른 스팸메일 필터링 방법은 비단 인터넷(Internet) 환경에서뿐만 아니라, 인트라넷(Intranet)이나 LAN(Local Area Network)을 사용하는 환경에서도 적용될 수 있음은 물론이다.

도 1은 본 발명이 적용되는 네트워크 환경에서 스팸 처리 엔진을 포함하는 전자메일 처리 시스템을 도시한

도면으로, 본 발명에 따른 전자메일 처리 시스템을 포함하는 네트워크 환경은 인터넷이나 인트라넷, 또는 LAN(40)에 접속할 수 있는 환경에 있는 클라이언트(Client) 서버(10), 사용자 단말기(로컬 PC, 웹 PC, 무선 인터넷 단말기 등) #1~N, 플랫폼(100), 웹서버(200), 메일서버(300), 및 데이터베이스(400)로 구성될 수 있다. 여기서는 이러한 네트워크 환경 중에서 인터넷을 사용하는 전자메일 시스템을 포함하는 네트워크 환경에 대하여 설명한다.

상기 클라이언트 서버(10)나 상기 사용자 단말기 #1~N(20 또는 30)은 전용선이나 다이얼-업(Dial-Up) 모뎀, ISDN, 이동통신 단말기를 통해 웹에 접속되면 상기 플랫폼(100)을 통해 상기 웹서버(200)나 메일서버(300)에 접속할 수 있으며, 상기 클라이언트 서버(10)나 상기 사용자 단말기 #1~N(20 또는 30)이 상기 메일서버(300)에 접속하기 위해서는 웹(Web), SMTP(Simple Mail Transfer Protocol)나 POP3(Post Office Protocol Version 3)의 프로토콜을 이용하면 된다..

상기 플랫폼(Multi-platform)(100)은 상기 클라이언트 서버(10)나 상기 사용자 단말기 #1~N(20 또는 30)이 상기 웹서버(200)나 상기 메일서버(300)에 원활하게 접속할 수 있도록 웹, SMTP, POP3프로토콜을 이용하는 다수의 접속 플랫폼을 지원하게 된다.

상기 웹서버(200)는 서버 또는 사용자(user) 환경의 클라이언트가 접속할 수 있는 고유의 URL(Uniform Resource Locator)를 가지며, 웹 서비스를 위한 제반 서비스를 담당한다. 특히 상기 웹서버(200)는 본 발명에 따른 스팸메일 필터링을 위한 스팸 처리 엔진(220)을 장착한다.

상기 메일서버(300)는 본 발명에 따른 전자메일 시스템으로 이루어지며, 상기 플랫폼(100)을 통해 접속된 서버 또는 사용자 환경의 클라이언트에게 전자메일과 관련된 서비스인 메일 보내기(Mail Sending), 메일 수신(Mail Receiving), 메일 읽기(Mail Reading) 등의 서비스를 제공한다. 특히 상기 메일서버(300)는 스팸 처리 엔진(220)에 의하여 본 발명에 따른 스팸메일 필터링을 제공받게 된다. 상기 메일서버(300)는 멀티-스레드(Multi-thread) 기반의 프로그램을 제공한다.

상기 스팸 처리 엔진(220)은 상기 웹서버(200)에 장착되며, 기존의 메일서버(300)와 웹서버(200)사이에서 상기 웹서버(200)를 통하여 상기 메일서버(300)로 송/수신되는 스팸메일을 차단하는 방화벽 역할을 수행한다. 상기 스팸 처리 엔진(220)의 기능은 도 2a 및 도 2b와 같다.

상기 도 2a는 본 발명의 일 실시 예에 따른 스팸 처리 엔진의 개념도이고, 도 2a는 본 발명의 다른 실시 예에 따른 스팸 처리 엔진의 개념도로서, 도시된 바와 같이 본 발명에 따른 스팸 처리 엔진은 전용 메일서버를 구비하는 상기 웹서버에 장착되어 웹서버를 통하여 메일서버로 송/수신되는 전자메일들 중 스팸메일을 필터링한다. 또한 전용 메일서버를 구비하지 않는 웹서버에 있어서 스팸메일 필터링뿐만 아니라 기본적인 메일서버의 기능을 제공한다.

도 3은 본 발명의 바람직한 실시 예에 따른 전자메일 처리 시스템의 계층 구성을 도시한 도면으로, 외부 사용자 및 서버와 연결되는 웹과 POP3 및 SMTP를 포함하는 플랫폼과, 바이러스 검출엔진 및 스팸 처리 엔진이 기본적인 메일 송/수신 기능을 수행하는 메일 엔진 위에 탑재된 계층 형태를 이룬다.

이와 같은 상기 전자메일 처리 시스템에서 본 발명에 따른 웹서버(200)의 내부 구성을 도 4를 통해 상세히 설명한다. 도 4는 본 발명의 바람직한 실시 예에 따른 웹서버의 내부 구성을 도시한 도면으로, 본 발명의 바람직한 실시 예에 따른 웹서버(200)는 플랫폼(100)을 통하여 송/수신되는 전자메일에서 스팸메일을 처리하는 스팸 처리 엔진(220)과 바이러스메일을 검출하고 이를 치료하는 바이러스 검출엔진(230) 및 상기 스팸 처리 엔진(220)과 바이러스 검출엔진(230)의 제어 및 웹서버(200)의 전반적인 동작을 제어하는 웹서버 처리부(210)를 구비한다. 상기 스팸 처리 엔진(220)은 상기 스팸 처리부(221), 메일헤더 필터링부(222), 메일본문 필터링부(223), 메일연결 필터링부(224), SMTP명령어 필터링부(225), 필터링엔진 자동업그레이드부(227) 및 관리자도구(229)를 적어도 구비한다.

상기 스팸 처리 엔진(220)은 본 발명에 따른 전자메일 중 스팸메일 처리를 위한 엔진으로서, 상기 스팸 처리부(221)의 제어에 따라 상기 플랫폼(100)을 통하여 송/수신되는 메일을 상기 메일헤더 필터링부(222)에서 스팸메일의 헤더조건에 따라 차단토록 메일헤더 필터링을 수행하고, 상기 메일본문 필터링부(223)에서 스팸메일의 본문조건에 따라 차단토록 메일본문 필터링을 수행한다. 또한 상기 메일연결 필터링부(224)에서 스팸메일의 연결수조건에 따라 차단토록 연결 필터링을 수행하고, 상기 SMTP명령어 필터링부(225)에서 스팸메일의 SMTP명령어조건에 따라 차단토록 SMTP명령어 필터링을 수행한다.

상기 스팸 처리 엔진(220) 내부의 구성을 보다 상세히 설명하면, 상기 메일헤더 필터링부(222)는 스팸메일로 설정되어 있는 특정 도메인, IP주소를 갖는 전자메일에 대하여 동일한 헤더조건을 만족하면 이를 메일서버 이전에 미리 차단한다.

상기 메일본문 필터링부(223)는 스팸메일로 결정할 수 있도록 설정되어 있는 본문조건인 어휘들을 기준으로 하여 이와 관련된 스팸메일을 차단한다. 상기 본문조건은 성인용 광고메일 등 공서양속에 반하는 내용을 유추하게 하는 어휘들이 될 수 있다.

상기 메일연결 필터링부(224)는 스팸메일로 결정할 수 있도록 설정되어 있는 다수의 메일발송을 동시에 시도하는 동시 연결수에 대한 제한조건에 따라 필터링을 수행하며, 또한 단일시간당 동일한 메일발송을 반복적으로 시도하는 단위시간당 연결수에 대한 제한조건에 따라 필터링을 수행한다. 상기 연결수조건은 특정 시간동안 다수의 사용자에게 동일한 내용의 메일을 배포하기 위해 다수의 연결을 시도하는 메일을 차단하기 위한 동시 연결수조건과, 단위시간당 동일한 메일을 반복적으로 배포하기 위한 연결을 시도하는 메일을 차단하기 위한 단위시간당 연결수조건을 포함한다.

상기 동시 연결수조건은 메일을 배포하기 위해 동시에 메일서버와 연결을 시도하는 연결수를 제한하여 동시에 배포할 수 있는 메일의 양을 제한함으로써, 스팸으로 인하여 착신이 불가능하였던 정상적인 메일의 착신을 가능하게 하고, 메일서버의 부하를 감소시키는 병렬 적인 효과가 있다.

또한 상기 단위시간당 연결수조건은 다량의 메일을 배포하기 위해 동시 연결수를 제한조건까지 줄이는 대신에 반복적으로 발송하고자하는 동일한 메일을 단위시간당 체크하여 해당 제한조건에 따라 필터링함으로

써 메일서버의 부하를 감소시키는 직접 적인 효과가 있다.

상기 SMTP명령어 필터링부(225)는 외부 및 내부의 메일 송/수신 요청에 대하여 SMTP명령어 집합 및 명령어 순서, 응답코드를 검색하여 유효한 명령어가 불필요하게 반복되거나 올바르지 못한 명령어 순서를 갖는 경우, 이를 차단함으로써, 서버부하를 감소시키고 정상적인 작동을 수행하도록 한다.

한편, 본 발명에 따른 스팸메일 필터링을 위한 상기 스팸 처리 엔진의 관리 및 유지보수를 위한 관리자도구(229) 및 상기 스팸 처리 엔진의 각 필터링엔진이 업그레이드되는 경우, 업그레이드 엔진을 제공하는 웹 서버에 자동 접속하여 업그레이드를 자동으로 수행하는 필터링엔진 자동업그레이드부(227)를 구비한다.

상기 바이러스 검출엔진(230)은 송/수신되는 메일을 메일서버(300)에서 처리하기 이전에 메일의 첨부파일을 포함하여 바이러스 감염여부를 검사 및 치료한다. 상기 바이러스 검출엔진(230)은 상기 메일서버(300)에서도 구비될 수 있다.

상기 웹서버 처리부(210)는 상기 스팸 처리 엔진(220) 및 바이러스 검출엔진(230)에서 스팸메일 및 바이러스메일 필터링을 위한 정보를 상기 데이터베이스(400)로부터 읽어들여 제공하며, 또한 스팸메일 및 바이러스메일의 처리 결과를 저장한다.

상기 데이터베이스(Database)(400)는 웹 서비스 및 메일 서비스와 관련된 각종 데이터 및 프로그램 정보들을 보관하고 있다. 일 예로 상기 데이터베이스(400) 중에서 전자메일에 관련된 데이터베이스의 구성은 도 5의 구성과 같다.

상기 도 5는 본 발명의 바람직한 실시 예에 따른 스팸메일 처리를 위한 데이터베이스의 구성을 도시한 도면으로, 스팸메일헤더정보 데이터베이스(411), 스팸메일본문정보 데이터베이스(412), 스팸메일 연결수정보 데이터베이스(413) 및 스팸메일 SMTP명령어정보 데이터베이스(414) 등으로 구성되는 스팸메일 정보 데이터베이스(410)와, 바이러스메일 정보 데이터베이스(420), 정상메일 정보 데이터베이스(430), 사용자 정보 데이터베이스(440), 메시지 저장 데이터베이스(450), 첨부파일 저장 데이터베이스(460)를 구비한다.

상기 스팸메일헤더정보 데이터베이스(411)는 스팸메일헤더조건에 대하여 스팸메일로 설정되어 있는 특정 도메인, IP주소(예로써, 발신자/수신자 정보, 참조 정보3, 보낸 날짜 정보, 제목 정보, 첨부파일명 정보)를 저장하고 있다.

상기 스팸메일본문정보 데이터베이스(412)는 스팸메일로 결정할 수 있도록 설정되어 있는 본문조건인 어휘들을 저장하고 있다.

상기 스팸메일 연결수정보 데이터베이스(413)는 스팸메일로 결정할 수 있도록 설정되어 있는 다수의 메일 발송을 동시에 시도하는 동시 연결수 및 단일시간당 동일한 메일발송을 반복적으로 시도하는 단위시간당 연결수정보를 저장하고 있다.

상기 스팸메일 SMTP명령어정보 데이터베이스(414)는 외부 및 내부의 메일 송/수신 요청에 대하여 SMTP명령어 집합 및 명령어 순서, 응답코드를 저장하고 있다.

상기 정상메일 정보 데이터베이스(430)는 상기 스팸 처리 엔진(220)에서 스팸메일이 필터링된 후 정상적인 메일에 대한 제반 정보를 저장하고 있다.

상기 바이러스메일 정보 데이터베이스(420)는 바이러스 백신 프로그램을 저장하며, 각종 바이러스의 종류 및 이에 대한 치료 사항과 바이러스 치료결과 등의 바이러스 검사/치료에 필요한 제반 프로그램 및 데이터를 저장하고 있다.

상기 사용자 정보 데이터베이스(440)는 사용자들의 정보를 저장하고 있다.

상기 메시지 저장 데이터베이스(450)는 수신 또는 발신 전자메일 중에서 사용자에 의해 작성되는 메시지 내용 정보를 저장하고 있다.

상기 첨부파일 저장 데이터베이스(460)는 전자메일에 첨부되는 첨부파일의 정보 및 내용 정보를 저장하고 있다.

이외에도 상기 데이터베이스(400)는 상기 웹 서비스와 관련된 제반 데이터 및 소스 프로그램을 저장하고 있다.

도 6은 본 발명의 바람직한 실시 예에 따른 전자메일 처리 시스템에서 메일 수신 서비스를 도시한 도면이고, 도 7은 본 발명의 바람직한 실시 예에 따른 전자메일 처리 시스템에서 메일 발송 서비스를 도시한 도면이며, 도 8은 본 발명의 바람직한 실시 예에 따른 전자메일 처리 시스템에서 스팸 필터링 과정을 도시한 도면이다.

이하 상술한 도 1 내지 도 5 및 도 6 내지 도 8을 참조하여 본 발명의 바람직한 실시 예에 따른 전자메일 처리 시스템에서 스팸메일 필터링 방법을 설명한다.

먼저, 도 6을 참조하면, 메일 수신(600) 서비스는 먼저, 601단계의 용이한 접속을 위해 플랫폼(100)을 지원한다. 이렇게 지원되는 플랫폼(100)을 통해 603단계에서 상기 메일서버(300)의 제어부인 메일 처리부(미도시함)는 타 서버를 통해 메일이 수신되면 제어권을 상기 스팸 처리부(221)에 넘긴다.

그러면, 상기 스팸 처리부(221)는 수신된 메시지를 800단계에서 메시지를 재가공하게 되는데, 먼저 801단계에서 상기 스팸 처리부(221)는 상기 메일헤더 필터링부(222)를 제어하여 상기 스팸메일헤더정보 데이터베이스(411)의 정보에 따라 상기 수신되는 메일을 스팸메일의 헤더조건에 따라 차단하는 메일헤더 필터링 과정을 수행한다.

그리고 803단계에서 상기 스팸 처리부(221)는 상기 메일본문 필터링부(223)를 제어하여 상기 스팸메일본문정보 데이터베이스(412)의 정보에 따라 상기 메일헤더 필터링된 메일을 스팸메일의 본문조건에 따라 차단하는 메일본문 필터링 과정을 수행한다.

이어 805단계에서 상기 스팸 처리부(221)는 상기 메일연결 필터링부(224)를 제어하여 상기 스팸메일 연결 수정보 데이터베이스(413)의 정보에 따라 상기 메일본문 필터링된 메일을 스팸메일의 연결수조건에 따라 차단하는 연결 필터링 과정을 수행한다.

그리고 807단계에서 상기 스팸 처리부(221)는 상기 SMTP명령어 필터링부(225)를 제어하여 상기 스팸메일 SMTP명령어 정보 데이터베이스(414)의 정보에 따라 상기 연결 필터링된 메일을 스팸메일의 SMTP명령어조건에 따라 차단하는 SMTP명령어 필터링 과정을 수행한다.

그리고 809단계에서 상기 스팸 처리부(221)는 상기 바이러스 검출엔진(230)을 제어하여 상기 바이러스메일 정보 데이터베이스(420)의 정보에 따라 상기 SMTP명령어 필터링된 메일을 바이러스 검사 및 치료하는 과정을 수행한다.

이어 상기 메일 처리부(미도시함)는 605단계에서 필터링된 스팸메일에 대하여 스팸메일 정보 데이터베이스(410)의 각 해당 데이터베이스(411 내지 414)에 갱신 저장함과 아울러, 상기 필터링 후 정상 메일 정보를 상기 정상메일 정보 데이터베이스(430)에 저장하고, 메시지는 상기 메시지 저장 데이터베이스(450)에 저장하며, 첨부파일은 상기 첨부파일 저장 데이터베이스(460)에 저장하여 607단계에서 메일 수신을 종료한다.

도 7에 보인 바와 같이 상기 메일 발송 서비스(700)는 접속에서부터 메일 보내기 종료까지 크게 5단계로 수행되는데, 먼저 701단계에서 상기 메일서버(300)의 제어부인 메일 처리부(미도시함)는 DNS 내부 디코딩을 수행한다. 그리고 703단계에서 상기 메일 처리부는 사용자(20 또는 30)가 상기 플랫폼(100)을 지원하는 상기 메일서버(300)에 접속하면 705단계에서 통상의 사용자 인증과정을 수행한다. 상기 사용자 인증이 정상적으로 완료되면 상기 메일 처리부(미도시함)는 제어권을 상기 스팸 처리부(221)에 넘긴다.

상기 스팸 처리부(221)는 800단계에서 사용자에 의해 작성 완료된 메일(받는 사람, 참조, 내용, 첨부파일 등)을 송신 메일의 포맷에 맞도록 재가공한다. 이때, 상기 스팸 처리부(221)는 수신된 메시지를 800단계에서 메시지를 재가공하게 되는데, 먼저 801단계에서 상기 스팸 처리부(221)는 상기 메일헤더 필터링부(222)를 제어하여 상기 스팸메일헤더정보 데이터베이스(411)의 정보에 따라 상기 수신되는 메일을 스팸메일의 헤더조건에 따라 차단하는 메일헤더 필터링 과정을 수행한다.

그리고 803단계에서 상기 스팸 처리부(221)는 상기 메일본문 필터링부(223)를 제어하여 상기 스팸메일본문 정보 데이터베이스(412)의 정보에 따라 상기 메일헤더 필터링된 메일을 스팸메일의 본문조건에 따라 차단하는 메일본문 필터링 과정을 수행한다.

이어 805단계에서 상기 스팸 처리부(221)는 상기 메일연결 필터링부(224)를 제어하여 상기 스팸메일 연결 수정보 데이터베이스(413)의 정보에 따라 상기 메일본문 필터링된 메일을 스팸메일의 연결수조건에 따라 차단하는 연결 필터링 과정을 수행한다.

그리고 807단계에서 상기 스팸 처리부(221)는 상기 SMTP명령어 필터링부(225)를 제어하여 상기 스팸메일 SMTP명령어 정보 데이터베이스(414)의 정보에 따라 상기 연결 필터링된 메일을 스팸메일의 SMTP명령어조건에 따라 차단하는 SMTP명령어 필터링 과정을 수행한다.

그리고 809단계에서 상기 스팸 처리부(221)는 상기 바이러스 검출엔진(230)을 제어하여 상기 바이러스메일 정보 데이터베이스(420)의 정보에 따라 상기 SMTP명령어 필터링된 메일을 바이러스 검사 및 치료하는 과정을 수행한다.

이후, 707단계에서 상기 메일 처리부(미도시함)는 메일을 발송하게 된다. 이때, DNS(Domain Name System) 내부 코딩 동작이 이루어지며, 파일의 입/출력(I/O) 시간을 줄이기 위해 발신메일 인덱스를 만들어 상기 스팸메일 연결수정보 데이터베이스(413)에 저장하여 메일 발송을 709단계에서 종료한다.

한편, 본 발명의 상세한 설명에서는 구체적인 실시 예를 들어 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능함은 물론이다. 그러므로 본 발명의 범위는 설명된 실시 예에 국한되어 정해져서는 안되며 후술하는 특허청구의 범위뿐 아니라 이 특허청구의 범위와 균등한 것들에 의해 정해져야 한다.

발명의 효과

상술한 바와 같이 본 발명은 전자메일 처리 시스템에서 송/수신되는 메일을 처리하는 메일서버의 부하를 최소화할 수 있는 이점이 있다. 또한 본 발명은 웹메일서버 및 메일전용 서버에 스팸메일을 폭넓게 차단할 수 있는 방화벽을 제공하는 효과가 있다.

(57) 청구의 범위

청구항 1

전자메일 처리 시스템에서 스팸메일을 필터링하는 방법에 있어서,

상기 전자메일 처리 시스템을 통하여 송/수신되는 메일을 스팸메일의 헤더조건에 따라 차단하는 메일헤더 필터링 과정과,

상기 메일헤더 필터링된 메일을 스팸메일의 본문조건에 따라 차단하는 메일본문 필터링 과정과,

상기 메일본문 필터링된 메일을 스팸메일의 연결수조건에 따라 차단하는 연결 필터링 과정과,

상기 연결 필터링된 메일을 스팸메일의 SMTP명령어조건에 따라 차단하는 SMTP명령어 필터링 과정과,

상기 SMTP명령어 필터링된 메일을 바이러스 검사 및 치료하는 과정을 적어도 구비함을 특징으로 하는 스팸

메일 필터링 방법.

청구항 2

제 1항에 있어서, 상기 연결 필터링 과정은,

상기 전자메일 처리 시스템이 다수의 메일발송을 동시에 시도하는 동시 연결수에 대한 제한조건에 따라 필터링을 수행함을 특징으로 하는 스팸메일 필터링 방법.

청구항 3

제 1항에 있어서, 상기 연결 필터링 과정은,

상기 전자메일 처리 시스템이 단일시간당 동일한 메일발송을 반복적으로 시도하는 단위시간당 연결수에 대한 제한조건에 따라 필터링을 수행함을 특징으로 하는 스팸메일 필터링 방법.

청구항 4

제 1항에 있어서, 상기 연결 필터링 과정은,

상기 전자메일 처리 시스템이 다수의 메일발송을 동시에 시도하는 동시 연결수에 대한 제한조건과, 상기 전자메일 처리 시스템이 단일시간당 동일한 메일발송을 반복적으로 시도하는 단위시간당 연결수에 대한 제한조건에 따라 필터링을 수행함을 특징으로 하는 스팸메일 필터링 방법.

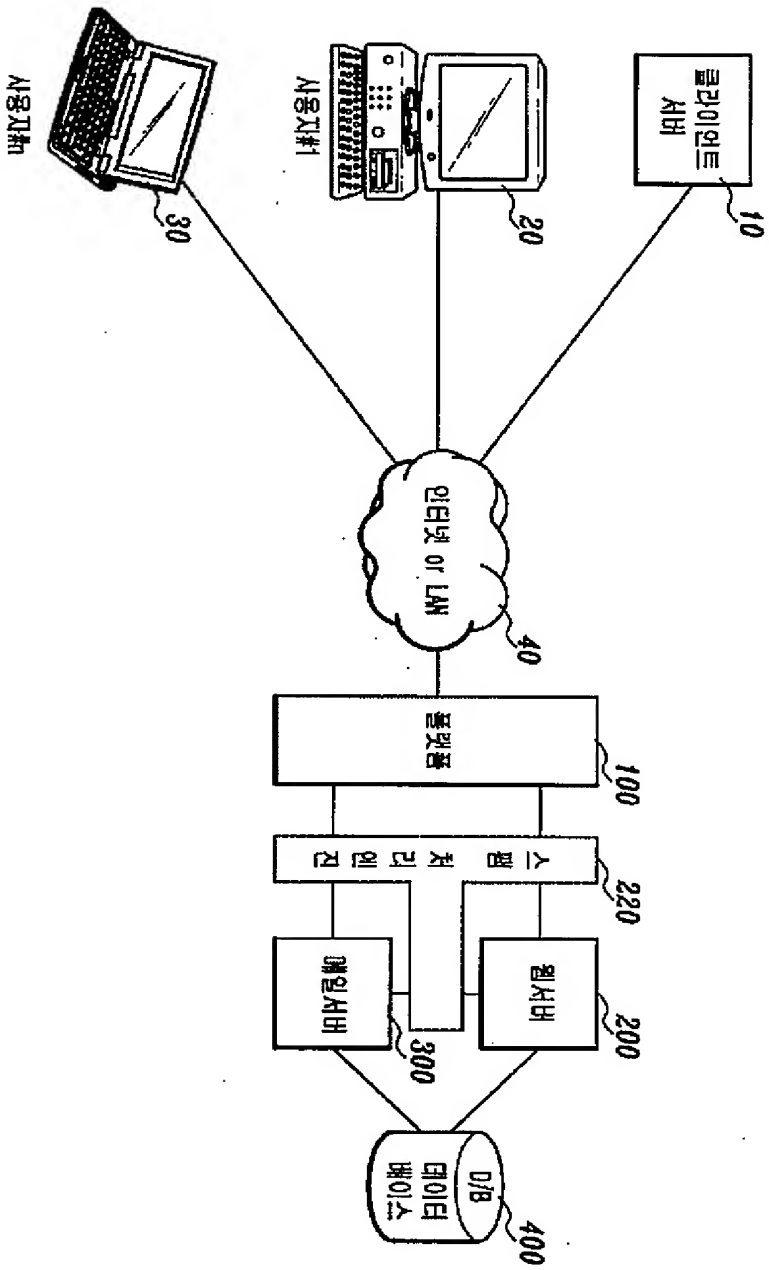
청구항 5

제 1항에 있어서,

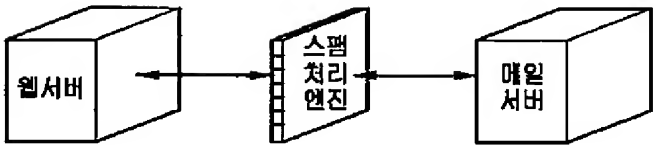
상기 전자메일 처리 시스템을 유지 및 보수하기 위한 관리자도구를 통하여 상기 모든 필터링 조건의 추가 변경이 가능함을 특징으로 하는 스팸메일 필터링 방법.

도면

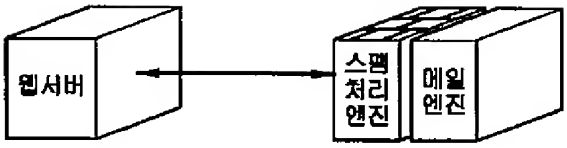
도면1


사용자n
사용자1
클라이언트 서버
30
20
10
인터넷 or LAN
40
플랫폼
100
시스템 관리 모듈
220
메일서버
300
웹서버
200
D/B 데이터베이스
400

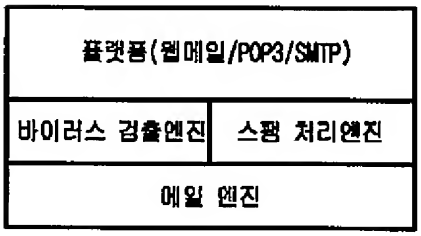
도면2a


웹서버
펌리진 스처엔
메일서버

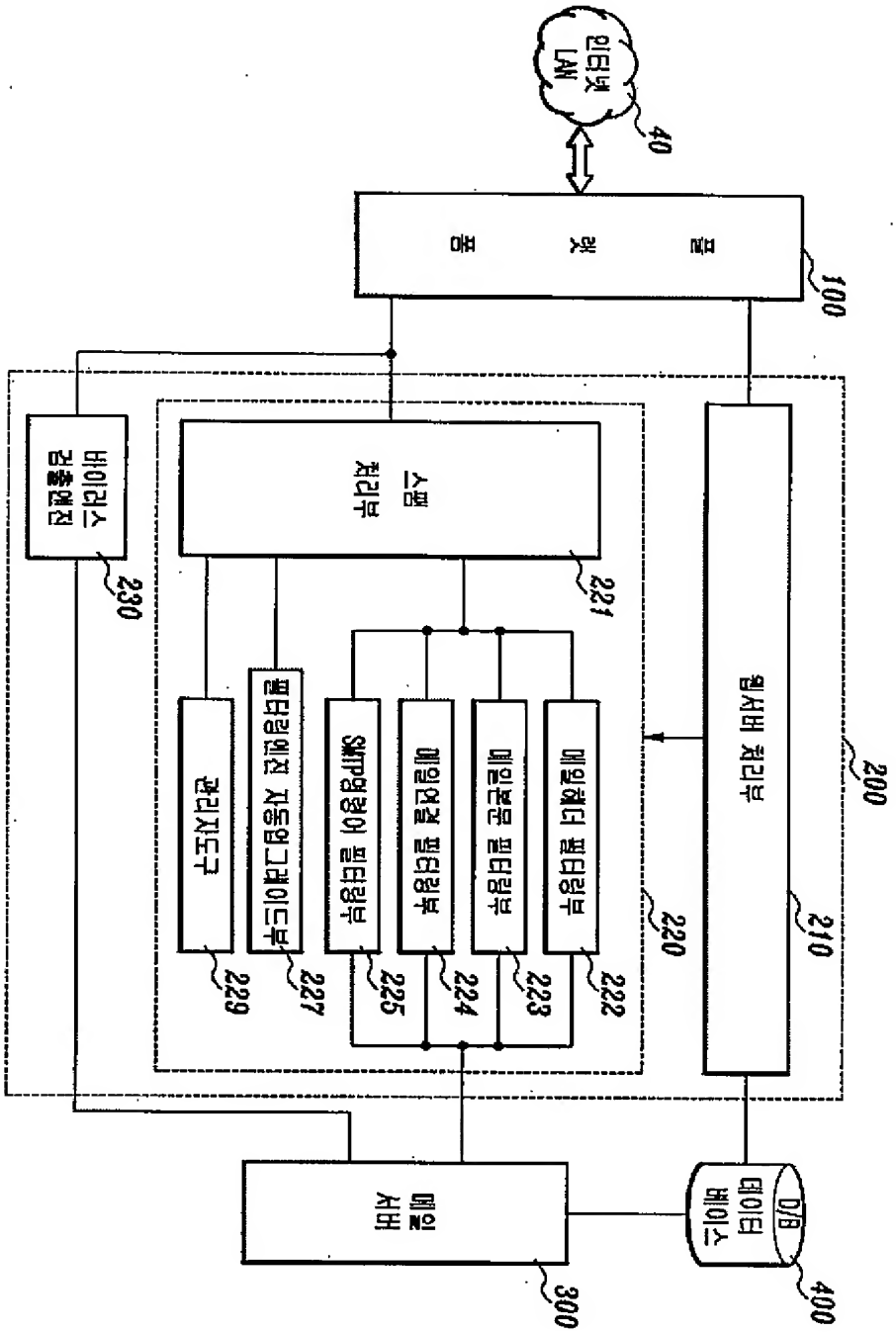
도면2b



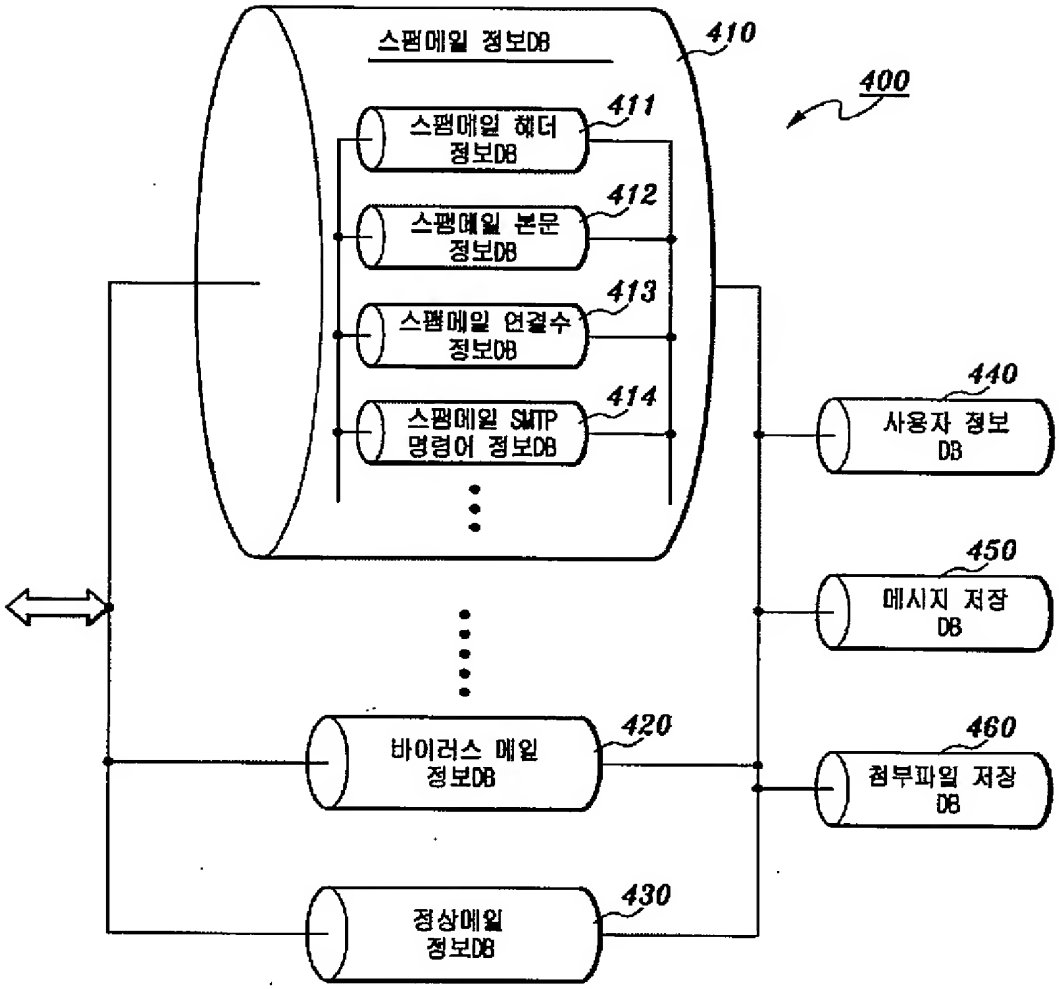
도면3



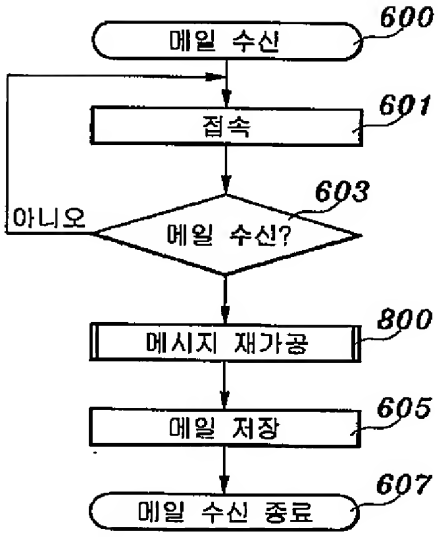
도면4


인터넷 LAN
40
통 신 부
100
웹서버 처리부
200
210
바이러스 검출처리
230
스풀 처리부
221
220
관리자도구
229
웹브라우저 기능업그레이드부
227
SMTP용어 프타일부
225
메일전달 프타일부
224
메일중계 프타일부
223
메일헤더 프타일부
222
메일 서버
300
D/B 데이터 베이스
400

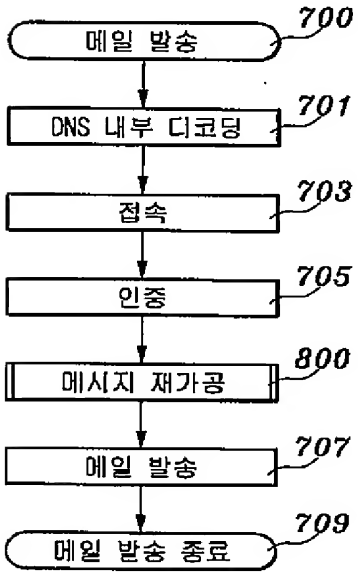
도면5


스팸메일 정보DB
410
400
411
스팸메일 헤더 정보DB
412
스팸메일 본문 정보DB
413
스팸메일 연결수 정보DB
414
스팸메일 SMTP 명령어 정보DB
440
사용자 정보 DB
450
메시지 저장 DB
420
바이러스 메일 정보DB
460
첨부파일 저장 DB
430
정상메일 정보DB

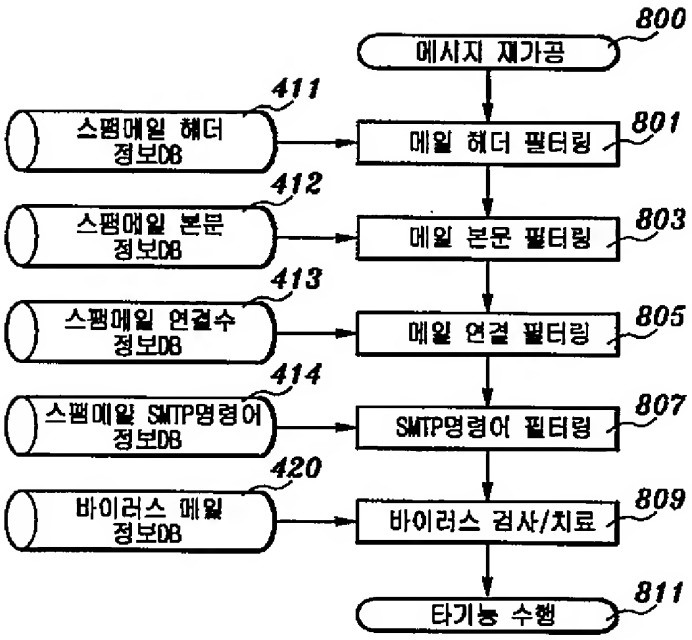
도면6


메일 수신
600
접속
601
아니오
메일 수신?
603
메시지 재가공
800
메일 저장
605
메일 수신 종료
607

도면7


메일 발송
700
DNS 내부 디코딩
701
접속
703
인증
705
메시지 재가공
800
메일 발송
707
메일 발송 종료
709

도면8


800
메시지 재가공
411
스팸메일 헤더 정보DB
801
메일 헤더 필터링
412
스팸메일 본문 정보DB
803
메일 본문 필터링
413
스팸메일 연결수 정보DB
805
메일 연결 필터링
414
스팸메일 SMTP명령어 정보DB
807
SMTP명령어 필터링
420
바이러스 메일 정보DB
809
바이러스 검사/치료
811
타기능 수행